Virginia Information Technologies Agency

# Chapter 28– Agency IT Procurement Security and Cloud Requirements for Solicitations and Contracts

## Chapter highlights

**Purpose**: This chapter provides information about the commonwealth's security and cloud compliance requirements for all agencies when procuring information technology (IT). VITA has statutory authority for the security of state government electronic information from unauthorized uses, intrusions or other security threats by developing and implementing policies, standards and guidelines, and providing governance processes and audits to ensure agency compliance.

**Key points**:

- Adherence to all information security policies, standards and guidelines is required of all state agencies and suppliers providing IT products or services to your agency.
- Also, any procurement of information technology made by the Commonwealth's executive, legislative, and judicial branches and independent agencies shall be made in accordance with federal laws and regulations pertaining to information security and privacy.
- In addition to VITA Security Standard SEC525-02, for any procurements for third-party (supplier-hosted) cloud services (i.e., Software as a Service), since agencies have $0 delegated authority to procure these types of solutions, there is a distinct process for obtaining VITA approval to procure.
- There are specially required Cloud Services terms and conditions that must be included in any solicitation or contract for cloud services  and a questionnaire that must be included in the solicitation for bidders to complete and submit with their proposals.

## Table of contents

## 28.0 Introduction

Virginia Information Technologies Agency (VITA), under the authority of § 2.2-2009 of the *Code of Virginia*, is directed to: ". . .  provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies."

Additionally, the 2017 General Assembly session included the following legislative changes regarding VITA's statutory security responsibilities:

- §2.2-2009 of the *Code of Virginia* requires the Chief Information Officer of the Virginia Information Technologies Agency to develop policies, standards, and guidelines to ensure that any procurement of information technology made by the Commonwealth's executive, legislative, and judicial branches and independent agencies is *made in accordance with federal laws and regulations pertaining to information security and privacy*.
- In accordance with §2.2-2009 of the *Code of Virginia*, the Virginia Information Technologies Agency shall operate an information technology security service center to support the information technology security needs of agencies electing to participate in the information technology security service center. Support for participating agencies shall include, but not be limited to, vulnerability scans, information technology security audits, and Information Security Officer services. Participating agencies shall cooperate with the Virginia Information Technologies Agency by transferring such records and functions as may be required.
- Established funding for both Technology Security Oversight Services and Cloud Based Services Oversight (refer to Title 2.2, Chapter 20.1 of the *Code of Virginia*).

The CIO has given VITA's Commonwealth Security and Risk Management (CSRM) Division responsibility for developing the security-related policies, standards and guidelines, implementing them and providing governance processes and audits to ensure agency compliance. VITA's Project Management Division (PMD) and Supply Chain Management Division (SCM) and other VITA divisions participate in various oversight and governance capacities to assist CSRM in fulfilling VITA's statutory security obligations.

## 28.1 VITA Information security policies, standards and guidelines (Security PSGs) required in all IT solicitations and contracts

### 28.1.1 Application of Security PSGs to all IT solicitations and contracts

All Security PSGs are available at this URL: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/. Adherence to the Security PSGs is required of all state agencies and suppliers providing IT products or services to your agency. Agency information security officers (ISO) or agency AITRs are familiar with them.

When developing an IT solicitation or contract, the agency procurement lead must ensure the above link is included in the Technical/Functional Requirements section of the document. Use the Minimum Requirements Matrix which you can download from this SCM webpage. It is located at the first bullet under the Forms section: https://www.vita.virginia.gov/supply-chain/scm-policies-forms/.

This matrix includes usable mandatory language that points to the Security PSGs link above, as well as mandatory language and links to other VITA PSGs that cover Enterprise Architecture requirements, Data Standards requirements and IT Accessibility and 508 Compliance requirements. Your procurement's project manager, ISO or AITR will know if any formal exceptions will be needed and will obtain any such exception from VITA, should the supplier proposal not be able to comply with any of these requirements.

In addition, if a procurement is a cloud-based procurement (i.e., off-premise hosting), following VITA's selection of the best proposal(s) representing best value to the commonwealth, Supplier's failure to successfully answer, negotiate and/or comply with any resulting security exceptions that may arise in order to approve Supplier's cloud application, may result in removal from further consideration.

### 28.1.2 Application of VITA enterprise cloud oversight services (ECOS) policy and procedures to all SaaS solicitations and contracts

While agencies are required to comply with all Security PSGs as described in section 28.1.1, Security Standard SEC525-02 provides agency compliance requirements for non-CESC hosted cloud solutions.

In addition to Security Standard SEC525-02, for any procurements for third-party (supplier-hosted) cloud services (i.e., Software as a Service), agencies must use this process obtaining VITA approval to procure.  Refer to the Third Party Use Policy at this link: https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/ThirdPartyUsePolicy.pdf.

Your agency's Information ISO or AITR can assist you in understanding this process and in obtaining the required documentation to include in your solicitation or contract. There are specially required Cloud Services terms and conditions that must be included in your solicitation and contract, and a questionnaire that must be included in the solicitation for bidders to complete and submit with their proposals. You may also contact: enterpriseservices@vita.virginia.gov

More guidelines for application of ECOS is available here: https://www.vita.virginia.gov/services/service-catalog/cloud-and-oversight-services/enterprise-cloud-oversight-services-ecos.html

**Supply Chain Management Division (SCM) and other VITA divisions participate in various oversight and governance capacities to assist CSRM in fulfilling VITA's statutory security obligations.**